UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/844,439	04/30/2001	Yves Louis Gabriel Audebert	L741.01102	9088

7590 11/19/2004

STEVENS, DAVIS, MILLER & MOSHER, LLP
Suite 850
1615 L Street, N.W.
Washington, DC 20036

EXAMINER	
SON, LINH L D	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 11/19/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/844,439	AUDEBERT ET AL.	
	Examiner	Art Unit	
	Linh Son	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *04/30/2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *01/03, 10/01*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 1 recites the limitation "said second remote computer" in the claim. There is insufficient antecedent basis for this limitation in the claim. For the purpose of examination, Examiner assumes the "said second remote computer" means "said subsequent remote computer". Appropriate correction is necessary.

3. Claim 13 recites the limitation "Generating PSD algorithm transfer command" in the claim. There is insufficient antecedent basis for this limitation in the claim. For the purpose of examination, Examiner assumes the "Generating PSD algorithm transfer command" has the meaning of "generating the authentication requirements using the PSD authentication algorithm". Appropriate correction is necessary.

Claim Rejections - 35 USC § 102

4. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States

only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

1. Claim 7 is rejected under 35 U.S.C. 102(e) as being anticipated by Audebert, US Patent No. 6694436B1, hereinafter '436.

The applied reference has a common inventor, Audebert, with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 102(e) might be overcome either by a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not the invention "by another," or by an appropriate showing under 37 CFR 1.131.

5. As per claim 7, "A method for providing authentication over a network using a pre-established communications pipe comprising; generating an authentication challenge on a first remote computer system in a proper format for processing by a PSD, encrypting said properly formatted challenge using a pre-established cryptography method, transmitting said encrypted challenge through said pipe to said PSD, decrypting said encrypted challenge by said PSD using said pre-established cryptography method, generating an authentication response by said PSD using said decrypted challenge and at least one internal PSD algorithm, encrypting said authentication response using said pre-established cryptography method, transmitting said encrypted authentication response through said pipe to said first remote computer system, and decrypting said encrypted authentication response by said first remote

computer system using said pre-established cryptography method and authenticating said response by said first remote computer system using at least one internal authentication algorithms" is taught in '436 (Col 13 lines 30 to Col 14 line 10).

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

1. Claims 1-6, and 8-17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Audebert, US Patent No. 6694436B1, hereinafter '436, in view of UHLER et al, US Pub No. US 20010039587A1, hereinafter '587.

2. As per claims 1-2, a system for providing authentication over a network using a pre-established communications pipe, comprising at least one client, at least one PSD, at least one first remote computer system and at least one subsequent remote computer system. said at least one client, further comprising: means for transferring incoming commands sent from said first remote computer system through said pipe to said PSD, means for transferring outgoing responses generated by said PSD to said first remote computer through said pipe, wherein said client is functionally connected to said PSD and said network and is functionally communicating over said pipe with a first

remote computer system" is taught in '436 (Col 9 lines 10-28, and Col 15 line 40 to Col 16 line 8); "said at least one PSD further comprising: at least one embedded PSD authenticating means, means to respond to at least one incoming command, means to generate an outgoing authentication response, means to transfer said authenticating means through said client to said first remote computer system, cryptography means for decrypting said incoming commands and encrypting said outgoing responses, wherein said PSD is functionally connected and is functionally communicating with said client and said first remote computer system" is taught in '436 (Col 13 line 30 to Col 14 line 10, and Col 17 lines 7-25); "said at least one first remote computer system further comprising: means of generating outgoing commands in a proper protocol for communicating with said PSD through said pipe, a first authenticating means for authenticating said PSD responses, cryptography means for decrypting said incoming responses and encrypting said outgoing commands, storage means for storing said authenticating means transferred from said PSD, wherein said first remote computer system is functionally connected to said network and is functionally communicating with said client and said PSD using said communications pipe" is taught in '436 (Col 13 line 30 to Col 14 line 10). However, "a second authenticating means using said PSD authenticating means to provide authentication response to said subsequent remote computer system; and said at least one subsequent remote computer system further comprising: means to generate authentication challenges, a third authenticating means for authenticating responses received over said network from said first remote computer system, wherein said second remote computer system is functionally connected to said

network and is in functional communications with said first remote computer system; and at least one network wherein said network includes means for functionally connecting and communicating with at least one client and one or more remote computer systems" is not taught in '436. Nevertheless, in '587 Uhler et al discloses a method and apparatus to access the remote servers utilizing smart card (Para 0072-73). The system in '587 comprises a personal computer with a smart card reader, the first remote computer (proxy server), and multiple subsequent remote computers (See Figure 2). The proxy server is the concentration point for all users and the first secure authentication layer to access a service. The proxy server receives the encrypted requests and forwards the authenticating data to the authentication server to verify and to authorize the request by means of transmitting the encrypted authorization back to the PSD or the smart card terminal (Para 0011-12, Para 0062-63, and Para 0081-0096). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate the subsequent remote computer to authenticate the PSD. Having layers of authentication mechanism will prevent fraudulence act to a network or service.

3. As per claims 3, 9, and 14, the system according to claims 1 or 2, 7, and 14 wherein said communications employs an open protocol" is taught in '436 (Col 21 lines 14).

4. As per claims 4, 10, and 15, the system according to claims 1 or 2, 7, and 14 wherein said communications employs a secure protocol" is taught in '436 (Col 12 lines 56-63).

5. As per claims 5, 11, and 16, "the system according to claims 1 or 2, 7, and 14 wherein said cryptography employs asynchronous methods" is taught in '436 (Col 23 lines 45-50).

6. As per claims 6, 12, and 17, "the system according to claims 1 or 2, 7, and 14 wherein said cryptography employs synchronous methods" is taught in '436 (Col 23 lines 45-50).

7. As per claim 8, "the method according to claim 7, further comprising; redirecting subsequent authentication challenges received over said network to said first remote computer system, processing said subsequent authentication challenges in said proper format for processing by a PSD through said pipe, encrypting said properly formatted challenge using said pre-established cryptography method transmitting said encrypted challenge through said pipe to said PSD, decrypting said encrypted challenge by said PSD using said pre-established cryptography method, generating an authentication response by said PSD using said decrypted challenge and at least one internal PSD algorithm, encrypting said authentication response using said pre-established cryptography method, transmitting said encrypted authentication response through said

pipe to said first remote computer system, decrypting said encrypted authentication response by said first remote computer system using said pre-established cryptography method" is taught in '436 (Col 13 line 30 to Col 14 line 10). However, "the routing said authentication response over said network to said subsequent remote computer system, authenticating said response by said subsequent remote computer system using at least one internal authentication algorithms" is not taught in '436. Nevertheless, in '587 Uhler et al discloses the "Method and Apparatus for Accessing Devices on a Network" invention, which include a subsequent remote server that contain the authentication data for verification requests routed from the proxy server. Similar to the Server Ssec in '436, the proxy server servers as the entrance point to a network to validate all incoming request as appropriate utilize the authentication server (the subsequent remote server) (Para 0011-12, Para 0062-63, and Para 0081-0096). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate the subsequent remote server to authenticate the request. Having a separate processor to authenticate the request will lessen the burden on the first remote computer, which is the concentration point of the network.

8. As per claim 13, "a method for providing authentication over a network using a pre-established communications pipe comprising: generating a PSD algorithm transfer command on a first remote computer system in a proper format for processing by a PSD, encrypting said properly formatted transfer command using a pre-established cryptography method, transmitting said encrypted command through said pipe to said

PSD, decrypting said encrypted command by said PSD using said pre-established cryptography method, copying said PSD algorithm into an internal memory location, encrypting said PSD algorithm using said pre-established cryptography method, transmitting said encrypted PSD algorithm through said pipe to said first remote computer system, decrypting said encrypted PSD algorithm by said first remote computer system using said pre-established cryptography method and storing said PSD algorithm in a secure location" is taught in '436 (Col 13 lines 30-60). Further, the authentication mechanism is at the first remote server. The "receiving at least one remote authentication challenge over said network from at least one subsequent remote computer system by said first remote computer system, generating an authentication response by said first remote computer system using said stored PSD algorithm, transmitting said generated authentication response over said network to said subsequent remote computer system, and authenticating said response by said subsequent remote computer system using at least one internal authentication algorithms" is not taught in '436. Nevertheless, '436 does teach a method of authentication by receiving the authentication requirements by the first remote server (proxy server). The first remote server then forwards the authentication requirements to the subsequent remote server (the authentication server). The subsequent remote server authenticates the received authentication requirements data and then flags the first remote server to allow the request (Para 0062-63). Therefore, it would have been obvious at the time of the invention was made for one having ordinary skill in the art to incorporate the subsequent remote server to authenticate the request. Having a

separate processor to authenticate the request will lessen the burden on the first remote computer, which is the concentration point of the network.

Conclusion

9. Any inquiry concerning this communication from the examiner should be directed to Linh Son whose telephone number is (571)-271-3856.

10. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor Kim Y. Vu can be reached at (571)-272-3859. The fax numbers for this group are (703)-872-9306 (official fax). Any inquiry of general nature or relating to the status of this application or proceeding should be directed to the group receptionist whose telephone number is (571)-272-2100.

11. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval IPAIR.I system. Status information for published applications may be obtained from either Private PMR or Public PMR. Status

information for unpublished applications is available through Private PMR only. For more information about the PAIR system, see http://pzr-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

GILBERTO BARRÓN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Linh LD Son

Patent Examiner